BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

Claims

[c1] 1. A system for determining communications events, comprising:

a key server to release keys to communicating parties, wherein said keys are encryption keys to encrypt or decryption keys to decrypt the communications and said communicating parties include originators seeking to create and recipients seeking to view the communications; and

for each of the communications, said key server also to:

assign an identifier;

store a record in a database that includes said identifier, a respective said decryption key, and respective controlling events;

receive zero, one, or more requests for said decryption key, wherein said requests include said identifier; and

determine at least one member of the set consisting of positive events and negative events based on said controlling events and how many said requests are received or when any said requests are received.

[c2] 2. The system of claim 1, wherein said encryption key and said decryption key are the same.

[c3] 3. The system of claim 1, wherein said encryption key and said decryption key are different.

[c4] 4. The system of claim 1, wherein said key server is able to generate said keys.

[c5] 5. The system of claim 1, wherein said key server is able to receive said keys from an outside source.

[c6] 6. The system of claim 5, wherein said outside source is a said originator.

[c7] 7. The system of claim 1, wherein said key server requires an assertion before releasing said keys.

[c8] 8. The system of claim 1, wherein at least some of said controlling events are defined based on attributes provided by said originator.

[c9] 9. The system of claim 1, wherein at least some of said controlling events are pre-stored in said database in anticipation of use in later said communications.

[c10] 10. The system of claim 9, wherein at least some of said controlling events are determined based on attributes received from a party other than a said originator.

[c11] 11. The system of claim 1, wherein a said controlling event specifies a time after which a said decryption key is made releasable, thereby specifying a delay before a said recipient can decrypt a said communication.

[c12] 12. The system of claim 1, wherein a said controlling event specifies a time after which a said decryption key is made un-releasable, thereby specifying an expiration after which a said recipient can no longer decrypt a said communication.

[c13] 13. The system of claim 1, wherein a said controlling event specifies how many times a said decryption key should be released to a said recipient,

thereby limiting the times said recipient can decrypt a said communication.

[c14] 14. The system of claim 1, wherein:

said key server requires an assertion for a said recipient; and

said controlling events specify at least one condition that must be met before releasing a said decryption key to said recipient.

[c15] 15. The system of claim 1, wherein said key server communicates data about at least one of said positive events or said negative events to at least one of said originator and another entity.

[c16] 16. The system of claim 15, wherein said another entity is a notification server.

[c17] 17. A method for determining communication events, the method comprising:

(a) receiving a first request for a resource ID to identify the communication, wherein said first request includes at least one identity of an intended recipient of the communication;

(b) defining at least one controlling event, wherein said controlling events include said at least one identity;

(c) providing said resource ID in reply to said first request;

(d) storing said resource ID, said controlling events, and a decryption key to decrypt the communication;

(e) monitoring for a second request for said decryption key, wherein said second request includes said resource ID and identifying information for a putative said intended recipient;

(f) if a said second request is received, then determining whether it conforms with said controlling events, and

(1) if so:

(i) providing said decryption key in reply to said second request; and

(ii) storing said identifying information and a positive event in association with said resource ID;

(2) else, storing a negative event in association with said resource ID; and

(g) alternately, if no said second request is received for a said intended recipient, then storing a negative event in association with said resource ID.

[c18] 18. The method of claim 17, wherein said step (c) includes providing an encryption key.

[c19] 19. The method of claim 18, wherein said encryption key and said decryption key are the same.

[c20] 20. The method of claim 18, wherein said encryption key and said decryption key are different.

[c21] 21. The method of claim 17, wherein said first request includes an authentication assertion and said step (a) includes verifying said authentication assertion before providing said resource ID in said step (c).

[c22] 22. The method of claim 17, wherein at least some of said controlling events are defined based on attributes provided by an originator of the

communication.

[c23] 23. The method of claim 17, wherein at least some of said controlling events are pre-stored before said step (a) in anticipation of later use in the communication.

[c24] 24. The method of claim 23, wherein at least some of said controlling events are determined based on attributes received from a party other than said originator.

[c25] 25. The method of claim 17, wherein a said controlling event specifies a time after which said decryption key is made releasable to a said recipient.

[c26] 26. The method of claim 17, wherein a said controlling event specifies a time after which said decryption key is made un-releasable to a said recipient.

[c27] 27. The method of claim 17, wherein a said controlling event specifies how many times said decryption key should be released to a said recipient.

[c28] 28. The method of claim 17, wherein said second request includes an authentication assertion including said identifying information and step (f) includes verifying said authentication assertion before providing said decryption key.

[c29] 29. The method of claim 17, further comprising a step (h) communicating data about at least one of said positive events or said negative events to at least one of an originator of the communication and another entity.

[c30] 30. The method of claim 29, wherein said another entity is a notification

server.